UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/644,841	08/21/2003	Yaron Mayer		6146

7590 02/09/2009

YARON MAYER
21 AHAD HA'AM ST.
JERUSALEM, 92151
ISRAEL

EXAMINER	
LANIER, BENJAMIN E	
ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
02/09/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/644,841	MAYER ET AL.	
	Examiner	Art Unit	
	BENJAMIN E. LANIER	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 January 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *See Continuation Sheet* is/are pending in the application.

4a) Of the above claim(s) *13,14,22,37,54,56* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,9-12,15,16,19,20,30,33,38,41-43,45,46,50-52,58,60-64 and 66-94* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Continuation of Disposition of Claims: Claims pending in the application are 1-5,9-12,15,16,19,20,30,33,38,41-43,45,46,50-52,58,60-64 and 66-94.

DETAILED ACTION

Response to Amendment

1. Applicant's amendment filed 09 January 2009 amends claims 1, 9, 16, 20, 28, 33, 41-43, 86, and 87. Applicant's amendment has been fully considered and entered.

Election/Restrictions

2. This application contains claims 13, 14, 22, 37, 54, and 56 drawn to an invention nonelected without traverse in the reply filed on 18 July 2008. A complete reply to the final rejection must include cancellation of nonelected claims or other appropriate action (37 CFR 1.144) See MPEP § 821.01.

Response to Arguments

3. Applicant argues, "Kardach…talks in paragraph [0032] about…a real-time kernel to run underneath an operating system that does not have real-time attributes. **However he does not say anything about implementing an area or ring below ring 0 which is more privileged than ring 0, and he does not talk a more privileged area or ring within ring 0 in which a control system and/or security system is adapted to catch exceptions caused by device drivers in ring 0 and/or by the operating system, and in fact he does not even mention ring 0 or rings or privilege levels at all anywhere in the patent.**" This argument is not persuasive because Applicant's claims define ring 0 as belonging to the operating system. Kardach discuses a real-time kernel running underneath of the operating system (ring 0 as defined by Applicant). Therefore, Kardach clearly discusses a privilege/ring level below ring 0.

4. Applicant argues, "Gaul does not talk at all about Copy-on-Write as in claims 86 & 87." In response, the features discussed by Applicant are taught by Nachenberg. Gaul was never

relied upon to teach the above mentioned claim limitations (See paragraph 17 of the previous Office Action).

5. Applicant argues, "Nachenberg…merely talk [sic] about emulating a program in a virtual environment to check if it is a virus. These lines do not talk at all for example about the features of claims 20 & 83 (which talk about identifying if the user or an application initiated an activity and [sic] acting differently accordingly)." This argument is not persuasive because Nachenberg discusses that the emulator can detect a file open operation (Col. 4, lines 8-9), which would be considered accessing a file outside the virtual environment of the program, and at least one potential security-risk command which is at least partially related the disk or other non-volatile storage device. Examiner would additionally like to point out that the Applicant is responsible for reviewing the content of all cited reference. The Office Action citations are merely a guide.

6. Applicant's arguments with respect to claims 46, 70-75, 77-82, 86, 90-93, do not comply with 37 CFR 1.111(c) because they do not clearly point out the patentable novelty which he or she thinks the claims present in view of the state of the art disclosed by the references cited or the objections made. Further, they do not show how the amendments avoid such references or objections.

7. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., automatic detection and warning the user about misusing resources) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

8. Applicant argues, "col. 1, lines 43-55 in Pitt…do not cover the features of claim 52, such as that the security system attaches to each message an identification that shows if the OS or another application is the source of the message, and the Security System allows certain message to be initiated only by the OS." This argument is not persuasive because Pitt (Col. 1, line 30 – Col. 2, line 16) clearly identifies that the dialog boxes originate from the operating system and therefore include an identification that shows the OS is the source.

9. Applicant argues, "Togawa…only talks about saving files in a save data area." This limitation is not persuasive because Togawa discloses any changes that happen on at least one of the hard disk and other nonvolatile storage devices and other connected media are completely undo-able at least for a certain time period, by keeping a rollback log of all changes or of all significant changes (Col. 17, lines 23-30).

10. Applicant's argument with respect to claim 66 is not persuasive because once a password protected file is accessed by the appropriate password; the computer hardware will allow access to the file.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

13. Claims 1-5, 9-12, 15, 16, 28, 30, 33, 41-43, 63, 94 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gaul, U.S. Publication No. 2001/0034847, in view of Kardach, U.S. 2002/0143845. Referring to claims 1, 9, 16, 28, 33, 41, 63, 94, Gaul discloses a remote security checking facility wherein a user at a terminal (Figure 1, 36) is authenticated to use a network security vulnerability testing application (Figure 1, 41), which meets the limitation of a control system and/or security system, the security system can identify strategic files and strategic directories using predefined rules. Gaul does not disclose that the vulnerability testing application runs below ring 0 or below the operating system of the terminal. Kardach discloses an application that runs below the operating system ([0032]), which meets the limitation of a computer system wherein at least one of device drivers and/or an operating system and/or parts of it are in ring 0 but there is at least one area or ring below ring 0 which is more privileged than ring 0, an operating system in ring 0 but there is at least one ring below ring 0 which is more privileged than ring 0, wherein there is a control system and/or security system which runs below the operating system. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the vulnerability testing application of Gaul to run below the operating system of the terminal in order to provide real-time alerts when the application discovers a vulnerability as taught by Kardach ([0031]-[0033]).

Referring to claims 2, 5, 10, 15, 30, Gaul discloses that the vulnerability testing application can test security features like intrusion detection ([0017]), which meets the limitation

of a monitoring and capturing system, which monitors at least one of storage devices and communications devices, a hardware element is used which monitors hardware accesses, so that the Security System and/or said hardware element can discover events where access has been made to at least one of storage devices and communication devices without an apparent corresponding event on the system level, any attempt to automatically generate an outgoing communication need explicit permission by the user, the security system automatically blocks potentially highly dangerous activities or asks the user for explicit authorization, even if the user supposedly allowed this to an application through the dialog box.

Referring to claims 3, 4, 11, 12, Gaul discloses that once security penetration testing completes, a recommendation report revealing the results is automatically delivered to the client ([0114]), which meets the limitation of said user interface at least also warns the user explicitly in cases of potentially highly dangerous activities, interception of more explicit warning of the user about potentially highly dangerous activities.

Referring to claims 42-43, Gaul discloses a remote security checking facility wherein a user at a terminal (Figure 1, 36) is authenticated to use a network security vulnerability testing application (Figure 1, 41), which meets the limitation of at least one part of the security system which runs on a specific computer becomes activated on said computer even if said computer is booted from at least one of a floppy drive, CD, network drive, and any other source that is not the normal boot area, said activation is done by at least one of the BIOS and the processor itself before the normal boot sequence begins.

14. Claims 19-20, 45-46, 51, 58, 60-61, 64, 67, 68, 70-75, 77-83, 86-93 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gaul, U.S. Publication No. 2001/0034847, in view of

Kardach, U.S. 2002/0143845, and further in view of Nachenberg, U.S. Patent No. 6,357,008. Referring to claims 19-20, 45, 51, 58, 60-61, 67, 70-75, 77-83, 86-93, Gaul does not disclose creating a virtual environment for programs. Nachenberg discloses creating a virtual environment for programs running on the computer terminal (Col. 3, line 62 – Col. 4, line 5), which meets the limitation of by default at least for some programs each program can only see itself and the operating system and the computer resources that it is allowed to see, so that it lives in a Virtual Environment (VE), the Security System is used by at least one user and the security system identifies if the application initiated at least one of accessing a file outside the virtual environment of the program, and at least one potential security-risk command which is at least partially related the disk or other non-volatile storage device, and so can allow more flexibility and/or less limitations and/or no limitations if the command was initiated directly by the user than if it was initiated by the application, if an application launches another application, the newly launched application is limited to the VE of the launching application, programs are allowed to send OS messages only to programs which are running within their own Virtual Environments, the security system prevents running processes from changing their code in memory, the security system also prevents applications from accessing directly lower level functions that can access hard disks and/or other devices except by calling them through the normal kernel interface, even if the user requested installation without VE limitation, the new program is first installed in a separate VE, and only after a certain time period or after the user authorizes it (and/or for example after the security system checks various parameters to see that things seem ok), the VE limitations are lifted or this VE is merged with the unlimited VE, at least in one mode and for at least some of the files and/or directories there is an indication near the file

and/or directory if it is a real file or a virtual file and/or the user and/or the administrator can see by clicking on the file and/or by the color of the file name or icon and/or by other indication, to which virtual environment it belongs, the security system filters or controls the communication between the two objects, segregation between programs and/or between virtual environments that is applied to at least one of hard disks and other storage media and/or other resources, wherein there are resources that are shared between virtual environments so that programs that are in a virtual environment are given the illusion that they are accessing said shared resources, but in reality if these programs make changes not explicitly allowed by the user in said shared resources, copy-on-write is used and/or said programs are redirected to another area so that said changes are only made in the virtual environment, at least for one or more shared resources and/or one or more programs and/or in one or more conditions if a program makes a change or changes in a shared resource, copy-on-write is used and/or said program is redirected to another area so that said changes are only make in the virtual environment and/or in said other area to which the program is redirected, the system enables the user to interact with an integrated view of the desktop and/or of the file system, based on merged views of virtual environments, so that the user can interact with programs that are in a virtual environment without having to switch to their virtual environment, automatic segregation between programs that is applied to at least one of the hard disks and other storage devices wherein files and directories are involved, automatic segregation between programs which the user can access, so that the directory structure in which a file is located automatically affects the access rights of other programs to it, capable of automatic segregation of programs into their natural environments so that by default programs are allowed to fully access files only within their natural environment, which is mainly the

directory in which the program is installed and its sub-directories, there are resources that are shared between virtual environments so that programs that are in a virtual environment are give the illusion that they are accessing said shared resources, but in reality if these programs make changes not explicitly allowed by the user in said shared resources, copy-on-write is used and/or said programs are redirected to another area sot that said changes are only made in the virtual environment, identifies if the user or an application initiated at least one of accessing a file outside the natural environment or virtual environment said application, and at least one potential security-risk command which is at least partially related to the hard disk or other non-volatile storage device, and so can allow more flexibility and/or less limitations and/or no limitations if the command was initiated directly by the user if it was initiated by the application, said copy-on-write and/or redirection to another area for making changes is used at least in one or more cases when a program does not have sufficient rights to make changes in one or more files or directories or other shared resources, "at least in one or more cases" means "at least for one or more programs", the program is automatically first installed in a separate VE even if the user did no request to install the program within a virtual environment, and only after a certain time period or after the user authorizes it, and/or after the security system checks various parameters to see that things seem ok, the VE limitations are lifted or this VE is merged with the unlimited normal environment, programs can be given the illusion that they have accessed shared keys in the registry, while in practice they are redirected each to its individual private file of relevant registry keys, said copy-on-write and/or redirection to another area for making changes is implemented at least when some programs need to install certain files in system directories, virtual shared directories are implemented by giving a program a logical view of the shared

directories or of only some of the files in it, so that if the program is allowed to see the file it sees the original copy, but if it changes files in the shared directory, said files will in reality be copied into files in the program's individual private area and changed only there. It would have been obvious to one of ordinary skill in the art at the time the invention was made for programs in Gaul to be implemented in a virtual environment in order to determine whether the program is malicious without risking infection as taught by Nachenberg, (Col. 3, line 62 – Col. 4, line 1).

Referring to claim 46, Gaul does not disclose scanning files for viruses. Nachenberg discloses scanning files for viruses (Col. 1, lines 27-38), which meets the limitation of if users download many files into a single download directory, the security system at least one of uses context sensitive information. It would have been obvious to one of ordinary skill in the art at the time the invention was made to scan for viruses in the system of Gaul in order to protect the system against infection as taught by Nachenberg (Col. 4, line 66 - Col. 5, line 4).

Referring to claim 64, Gaul does not disclose creating a virtual environment for programs. Nachenberg discloses creating a virtual environment for programs running on the computer terminal (Col. 3, line 62 – Col. 4, line 5) and identifying idle-loops in the emulated program (Col. 4, lines 25-31), which meets the limitation of automatically detecting by the software in the CPU itself entering the CPU into useless loops. It would have been obvious to one of ordinary skill in the art at the time the invention was made to scan for viruses in the system of Gaul in order to protect the system against infection as taught by Nachenberg (Col. 4, line 66 - Col. 5, line 4).

15. Claims 50, 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gaul, U.S. Publication No. 2001/0034847, in view of Kardach, U.S. 2002/0143845, and further in view of

Pitt, U.S. Patent No. 5,675,250. Referring to claims 50, 52, Gaul does not disclose replacing at least some of the operating system's dialogue boxes. Kardach discloses replacing at least some of the operating system's dialogue boxes (Col. 1, lines 43-55), which meets the limitation of the security system replaces at least some of the OS functions that deal with the OS message system, and attaches to each message an identification that shows if the OS or another application is the source of the message, and the security system allows certain messages to be initiated only by the OS. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the scanning system of Gaul to replace dialogue boxes in order to provide customized alert system as taught by Pitt (Col. 1, lines 46-52).

16. Claim 62 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gaul, U.S. Publication No. 2001/0034847, in view of Kardach, U.S. 2002/0143845, and further in view of Togawa, U.S. Patent No. 6,240,530. Referring to claim 62, Gaul does not disclose providing restoration of a hard disk or other nonvolatile storage devices for changes made over a certain period of time. Togawa discloses any changes that happen on at least one of the hard disk and other nonvolatile storage devices and other connected media are completely undo-able at least for a certain time period, by keeping a rollback log of all changes or of all significant changes (Col. 17, lines 23-30). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the system of Gaul to provide restoration of data in order to prevent destruction of data by viruses as taught by Togawa (Col. 17, lines 28-30).

17. Claim 66 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gaul, U.S. Publication No. 2001/0034847, in view of Kardach, U.S. 2002/0143845, and further in view of Moy, U.S. Patent No. 5,425,102. Referring to claim 66, Gaul does not disclose password

protecting files. Moy discloses password protecting files (Abstract), which meets the limitation of the hardware of the CPU and/or the hardware of the disk itself does not allow any access to a file unless the software that tries to access it is identified as its rightful owner, by at least one of provided the appropriate password, and other means. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the system of Gaul to provide password protection for files in order to provide access control security for data files as taught by Moy (Col. 1, line 20 – Col. 2, line 8).

18. Claim 69 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gaul, U.S. Publication No. 2001/0034847, in view of Kardach, U.S. 2002/0143845, and further in view of Luke, U.S. Patent No. 6,813,712. Referring to claim 69, Gaul does not disclose that the system monitors for unusual disk activity. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made for the system of Gaul to monitor for unusual disk activity because excessive hard drive activity is a symptom of virus infection as taught by Luke (Col. 4, lines 15-20).

19. Claims 76, 84 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gaul, U.S. Publication No. 2001/0034847, in view of Kardach, U.S. 2002/0143845, and further in view of Angelo, U.S. Patent No. 5,944,821. Referring to claims 76, 84, Gaul does not disclose preventing programs for unauthorized trapping of the keyboard device in order to catch keystrokes of other programs, in order to prevent theft of data from the user's hard disk or other non-volatile storage device. Angelo discloses a system that prevents programs from unauthorized trapping of the keyboard device in order to catch keystrokes of other programs, in order to prevent theft of data from the user's hard disk or other non-volatile storage device (Col. 11, lines 30-44). It would

have been obvious to one of ordinary skill in the art at the time the invention was made for the system of Gaul to prevent trapping of keystrokes in order to prevent user-entered data from being surreptitiously obtained as taught by Angelo (Col. 11, lines 35-38).

20. Claim 85 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gaul, U.S. Publication No. 2001/0034847, in view of Kardach, U.S. 2002/0143845, in view of Nachenberg, U.S. Patent No. 6,357,008, and further in view of Calder, U.S. Publication No. 2002/0065869. Referring to claim 85, Nachenberg does not disclose that the virtual environment includes an illusion of the root of a drive. Calder discloses that a virtual environment includes an illusion of the root of a drive ([0135]), which meets the limitation of at least one program is given the illusion that it installed itself on the root of a drive, but in fact it is installed in a lower directory. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the virtual environment of Nachenberg to includes an illusion of the root of a drive in order to provide the emulated program with the expected directory structure as taught by Calder ([0239]).

Conclusion

21. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN E. LANIER whose telephone number is (571)272-3805. The examiner can normally be reached on M-Th 7:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432